

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION of

LORTZ

Appln. No. 09/818,934

Group Art Unit: Unknown

Filed: March 28, 2001

Examiner: Unknown

Title: METHOD AND SYSTEM FOR MAPPING
NETWORK ATTACKS ONTO A STRATEGY GAME

July 6, 2001

PRELIMINARY AMENDMENT

Hon. Commissioner of Patents
Washington, DC 20231

Sir:

Prior to examination on the merits, kindly enter the following amendments:

IN THE CLAIMS:

Kindly replace pending claims 1-30 with the following claims:

1. (Amended) A method for mapping network attacks onto a strategy game, said method comprising:

receiving, by a transformer, at least one log file, generated by network security monitoring tools; and

transforming, by said transformer, said at least one log file into a set of characters with associated action inputs, wherein at least one of said characters is associated with an action input.

2. The method according to claim 1, wherein said network security monitoring tools include off-the-shelf network security monitoring tools.

09818934-070601

3. The method according to claim 1, wherein said at least one log file includes different types of vendor-specific log files, generated by corresponding vendor-specific network security monitoring tools.

4. (Amended) The method according to claim 1, further comprising:
converting, using at least one log file transformer agent, said at least one log file into one or more event representations; and
mapping, by a security event transformer agent, said one or more event representations to said set of characters and said associated action inputs.

5. The method according to claim 4, wherein said event representations include a vendor-independent representation.

6. The method according to claim 4, wherein each of said log file transformer agents corresponds to one of said network security monitoring tools and converts a type of log file generated by said one of said network security monitoring tools to said event representation.

7. (Amended) The method according to claim 4, wherein said converting comprises:
analyzing each of said at least one log file generated by one of said network security monitoring tools;

detecting one or more events based at least in part on the result from said analyzing; and

generating said one or more event representations for said one or more events.

8. (Amended) The method according to claim 4, wherein said mapping comprises:
processing said one or more event representations;

selecting a character for each of said event representations;
determining an action input associated with each of said selected characters based
at least in part on said each of said event representations; and
storing said character and said associated action input in a format as a game
session.

9. The method according to claim 8, wherein said format includes a saved session
format of a strategy game.

10. The method according to claim 1, further comprising:
rendering said set of characters and said associated action inputs in the form of a
strategy game; and
displaying a result of said rendering on a screen of a display unit.

11. A transformer for mapping network attacks onto a strategy game, said transformer
comprising:
a receiver configured to receive at least one log file generated by network security
monitoring tools; and
a transformer agent configured to transform said at least one log file into a set of
characters with associated action inputs, wherein each of said characters is associated with an
action input.

12. The transformer according to claim 11, wherein said network security monitoring
tools include off-the-shelf network security monitoring tools.

13. The transformer according to claim 11, wherein said at least one log file includes
different types of vendor-specific log files, generated by corresponding vendor-specific network
security monitoring tools.

14. (Amended) The transformer of claim 11, wherein said transformer agent comprises:

at least one log file transformer agent configured to convert said at least one log file into one or more event representations; and

a security event transformer agent configured to map said one or more event representations to said set of characters and said associated action inputs.

15. The transformer according to claim 14, wherein said event representations include a vendor-independent representation.

16. The transformer according to claim 14, wherein each of said log file transformer agents corresponds to one of said network security monitoring tools and converts a type of log file generated by said one of said network security monitoring tools to said event representation.

17. (Amended) The transformer according to claim 14, wherein said at least one log file transformer agent analyzes each of said at least one log file generated by one of said network security monitoring tools, detects one or more events based at least in part on the result from said analyzing, and generates said one or more event representations for said one or more events.

18. The transformer according to claim 14, wherein said security event transformer agent processes said one or more event representations, selects a character for each of said event representations, determines an action input associated with each of said characters, and stores said character and said associated action input in a format as a game session.

19. The transformer according to claim 18, wherein said format includes a saved session format of a strategy game.

20. A system for mapping network attacks onto a strategy game, said system comprising:

a transformer configured to receive at least one log file generated by network security monitoring tools, and to transform said at least one log file into a set of characters with associated action inputs, wherein each of said characters is associated with an action input; and

a strategy game rendering mechanism, said rendering mechanism configured to render said set of characters and said associated action inputs in the form of a strategy game.

21. The system according to claim 20, further comprising a display unit coupled to said strategy game rendering mechanism, said display unit having a screen configured to display said strategy game.

22. A computer-readable medium encoded with a plurality of processor-executable instructions for:

receiving, by a transformer, at least one log file, generated by network security monitoring tools; and

transforming, by said transformer, said at least one log file into a set of characters with associated action inputs, wherein each of said characters is associated with an action input.

23. The computer-readable medium according to claim 22, wherein said network security monitoring tools include off-the-shelf network security monitoring tools.

24. The computer-readable medium according to claim 22, wherein said at least one log file includes different types of vendor-specific log files, generated by corresponding vendor-specific network security monitoring tools.

25. (Amended) The computer-readable medium according to claim 22, further comprising processor-executable instructions for:

converting, using at least one log file transformer agent, said at least one log file into one or more event representations; and

mapping, by a security event transformer agent, said one or more event representations to said set of characters and said associated action inputs.

26. The computer-readable medium according to claim 25, wherein said event representations include a vendor-independent representation.

27. The computer-readable medium according to claim 25, wherein each of said log file transformer agents corresponds to one of said network security monitoring tools and converts a type of log file generated by said one of said network security monitoring tools to said event representation.

28. (Amended) The computer-readable medium according to claim 25, wherein said converting comprises:

analyzing each of said at least one log file generated by one of said network security monitoring tools;

detecting one or more events based at least in part on the result from said analyzing; and

generating said one or more event representations for said one or more events.

29. (Amended) The computer-readable medium according to claim 25, wherein said mapping comprises:

processing said one or more event representations;

selecting a character for each of said event representations;

determining an action input associated with each of said selected characters based at least in part on said each of said event representations; and

storing said character and said associated action input in a format as a game session.

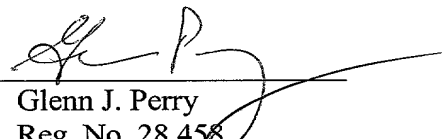
30. The computer-readable medium according to claim 29, wherein said format includes a saved session format of a strategy game.

REMARKS

Early and favorable action on the merits are respectfully requested.

Respectfully submitted,

PILLSBURY WINTHROP LLP

By: 
Glenn J. Perry
Reg. No. 28,458
Tel. No.: 703.905.2161
Fax No.: 703.905.2500

GJP/CMC/ded
1600 Tysons Boulevard
McLean, VA 22102
Tel. No.: 703.905.2000

Appendix

1. (Amended) A method for mapping network attacks onto a strategy game, said method comprising:

receiving, by a transformer, at least one log file, generated by network security monitoring tools; and

transforming, by said transformer, said at least one log file into a set of characters with associated action inputs, wherein [each] at least one of said characters is associated with an action input.

2. The method according to claim 1, wherein said network security monitoring tools include off-the-shelf network security monitoring tools.

3. The method according to claim 1, wherein said at least one log file includes different types of vendor-specific log files, generated by corresponding vendor-specific network security monitoring tools.

4. (Amended) The method according to claim 1, further comprising:

converting, using at least one log file transformer agent, said at least one log file into [zero] one or more event representations; and

mapping, by a security event transformer agent, said [zero] one or more event representations to said set of characters and said associated action inputs.

5. The method according to claim 4, wherein said event representations include a vendor-independent representation.

6. The method according to claim 4, wherein each of said log file transformer agents corresponds to one of said network security monitoring tools and converts a type of log file generated by said one of said network security monitoring tools to said event representation.

7. (Amended) The method according to claim 4, wherein said converting comprises:

analyzing each of said at least one log file generated by one of said network security monitoring tools;

detecting [zero] one or more events based at least in part on the result from said analyzing; and

generating said [zero] one or more event representations for said [zero] one or more events.

8. (Amended) The method according to claim 4, wherein said mapping comprises:

processing said one or more event representations;

selecting a character for each of said event representations;

determining an action input associated with each of said selected characters[, selected by said selecting,] based at least in part on said each of said event representations; and

storing said character and said associated action input in a format as a game session.

9. The method according to claim 8, wherein said format includes a saved session format of a strategy game.

10. The method according to claim 1, further comprising:

rendering said set of characters and said associated action inputs in the form of a strategy game; and

displaying a result of said rendering on a screen of a display unit.

11. A transformer for mapping network attacks onto a strategy game, said transformer comprising:

a receiver configured to receive at least one log file generated by network security monitoring tools; and

a transformer agent configured to transform said at least one log file into a set of characters with associated action inputs, wherein each of said characters is associated with an action input.

12. The transformer according to claim 11, wherein said network security monitoring tools include off-the-shelf network security monitoring tools.

13. The transformer according to claim 11, wherein said at least one log file includes different types of vendor-specific log files, generated by corresponding vendor-specific network security monitoring tools.

14. (Amended) The transformer of claim 11, wherein said transformer agent comprises:

at least one log file transformer agent configured to convert said at least one log file into [zero] one or more event representations; and

a security event transformer agent configured to map said [zero] one or more event representations to said set of characters and said associated action inputs.

15. The transformer according to claim 14, wherein said event representations include a vendor-independent representation.

16. The transformer according to claim 14, wherein each of said log file transformer agents corresponds to one of said network security monitoring tools and converts a type of log file generated by said one of said network security monitoring tools to said event representation.

17. (Amended) The transformer according to claim 14, wherein said at least one log file transformer agent analyzes each of said at least one log file generated by one of said network security monitoring tools, detects [zero] one or more events based at least in part on the result

from said analyzing, and generates said [zero] one or more event representations for said [zero] one or more events.

18. The transformer according to claim 14, wherein said security event transformer agent processes said one or more event representations, selects a character for each of said event representations, determines an action input associated with each of said characters, and stores said character and said associated action input in a format as a game session.

19. The transformer according to claim 18, wherein said format includes a saved session format of a strategy game.

20. A system for mapping network attacks onto a strategy game, said system comprising:

a transformer configured to receive at least one log file generated by network security monitoring tools, and to transform said at least one log file into a set of characters with associated action inputs, wherein each of said characters is associated with an action input; and

a strategy game rendering mechanism, said rendering mechanism configured to render said set of characters and said associated action inputs in the form of a strategy game.

21. The system according to claim 20, further comprising a display unit coupled to said strategy game rendering mechanism, said display unit having a screen configured to display said strategy game.

22. A computer-readable medium encoded with a plurality of processor-executable instructions for:

receiving, by a transformer, at least one log file, generated by network security monitoring tools; and

transforming, by said transformer, said at least one log file into a set of characters with associated action inputs, wherein each of said characters is associated with an action input.

23. The computer-readable medium according to claim 22, wherein said network security monitoring tools include off-the-shelf network security monitoring tools.

24. The computer-readable medium according to claim 22, wherein said at least one log file includes different types of vendor-specific log files, generated by corresponding vendor-specific network security monitoring tools.

25. (Amended) The computer-readable medium according to claim 22, further comprising processor-executable instructions for:

converting, using at least one log file transformer agent, said at least one log file into [zero] one or more event representations; and

mapping, by a security event transformer agent, said [zero] one or more event representations to said set of characters and said associated action inputs.

26. The computer-readable medium according to claim 25, wherein said event representations include a vendor-independent representation.

27. The computer-readable medium according to claim 25, wherein each of said log file transformer agents corresponds to one of said network security monitoring tools and converts a type of log file generated by said one of said network security monitoring tools to said event representation.

28. (Amended) The computer-readable medium according to claim 25, wherein said converting comprises:

analyzing each of said at least one log file generated by one of said network security monitoring tools;

detecting [zero] one or more events based at least in part on the result from said analyzing; and

generating said [zero] one or more event representations for said [zero] one or more events.

29. (Amended) The computer-readable medium according to claim 25, wherein said mapping comprises:

processing said one or more event representations;

selecting a character for each of said event representations;

determining an action input associated with each of said selected characters[, selected by said selecting,] based at least in part on said each of said event representations; and

storing said character and said associated action input in a format as a game session.

30. The computer-readable medium according to claim 29, wherein said format includes a saved session format of a strategy game.